ELECTRIC POWER RESEARCH INSTITUTE

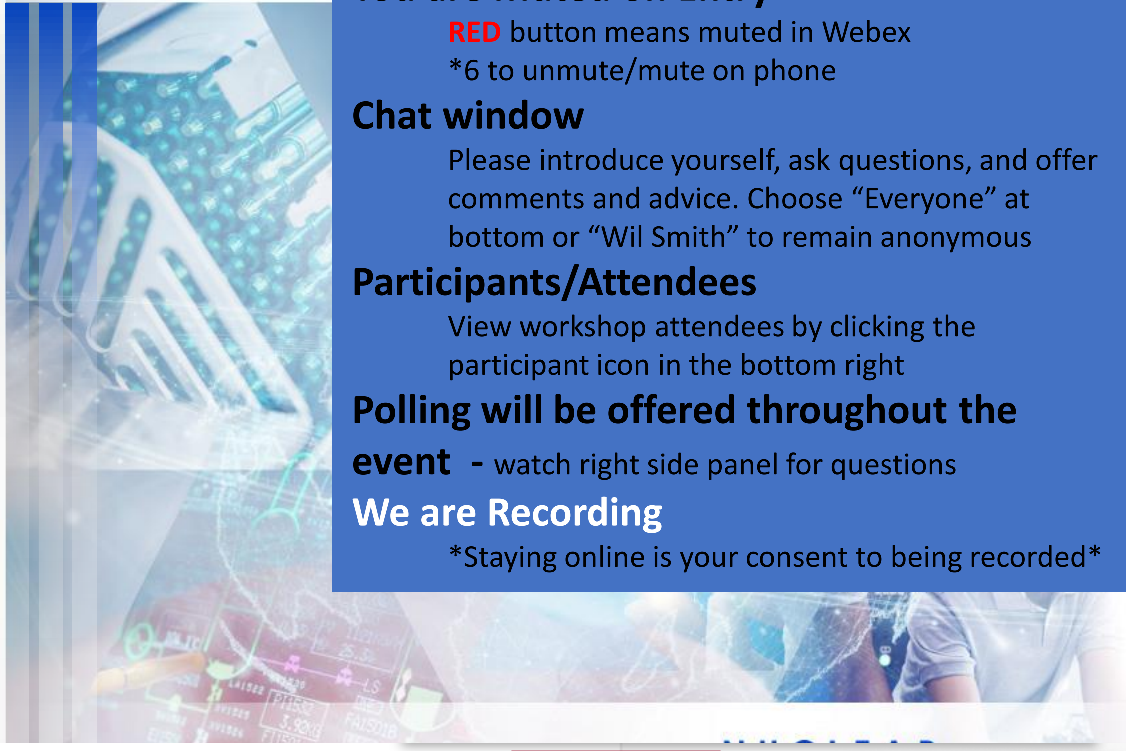
7th Annual EPRI-IEA Challenges in Energy Decarbonisation Expert Workshop

Big or Small: Decentralised Resources in a Decarbonised World

October 27-29, 2020

contacts:
David Hunter, dhunter@epri.com
Wil Smith, wsmith@epri.com
Keith Everhart, Keith.Everhart@iea.org

https://www.epri.com/pages/sa/washington-seminar
https://www.iea.org/past-events



Meeting Logistics

Audio Options:

1. Connect via computer audio
2. Have Webex call your phone

You are Muted on Entry

RED button means muted in Webex
*6 to unmute/mute on phone

Chat window

Please introduce yourself, ask questions, and offer comments and advice. Choose "Everyone" at bottom or "Wil Smith" to remain anonymous

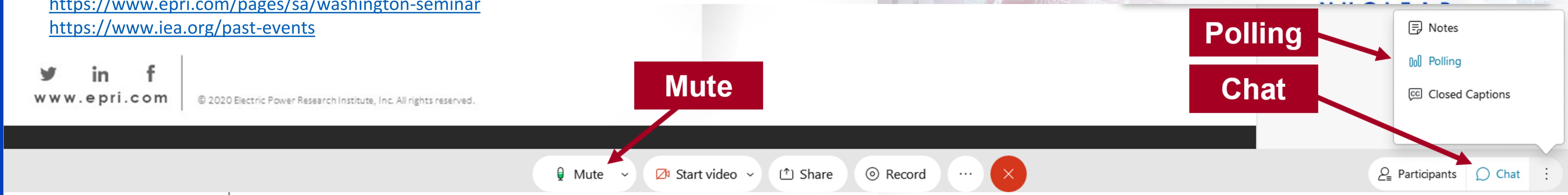
Participants/Attendees

View workshop attendees by clicking the participant icon in the bottom right

Polling will be offered throughout the event - watch right side panel for questions

We are Recording

Staying online is your consent to being recorded



Thursday, 29 October 2020

10:30 AM - 12:00 PM EST; 7:30 AM - 9:00 AM PST; 3:30 PM - 5:00 PM CET

Session 3: Reliability in a Decentralised System

The development of less centralized, more interconnected systems presents both new vulnerabilities as well as opportunities to improve reliability. What are these vulnerabilities and opportunities, and how can utilities, society, and governments best integrate central and distributed resources to create a more resilient system? In this session speakers will address implications to reliability of a future energy landscape split into central and decentral energy supply. *Followed by roundtable discussion.*

- Moderator: **César Alejandro Hernandez**, Head of Unit (Acting), Renewables Integration and Secure Electricity, IEA

Grid Reliability in a High Renewables World

- **Daniel Brooks**, Vice President, Integrated Grid and Energy Systems, EPRI

Using Distributed Resources to Keep Security of Supply

- **Róisín Quinn**, Head of National Control and Chief Engineer, National Grid ESO

Electric Vehicles and Grid Resiliency: Competing or Complementary?

- **Rob Chapman**, VP, Electrification & Sustainable Energy Strategy, EPRI

Australia Perspective

- **Barry O'Connell**, Principal Engineer Future Energy Systems, AEMO

Cybersecurity and Resilience

- **Amro Farid**, Associate Professor of Engineering, Dartmouth College

ELECTRIC POWER
RESEARCH INSTITUTE

Reliability in a High Renewables World

Daniel Brooks, PE
Vice President, Integrated Grid and Energy Systems

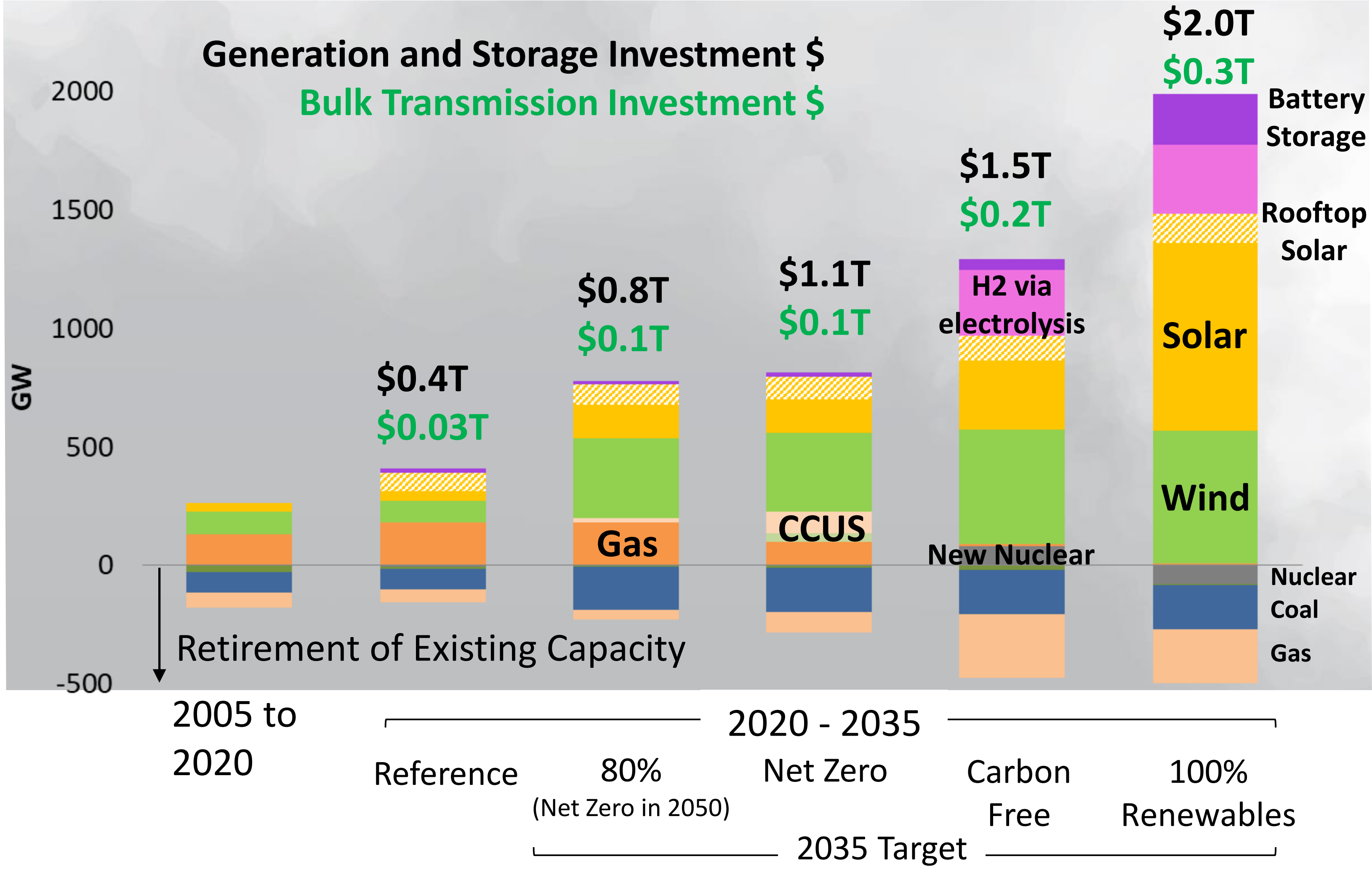
EPRI/IEA Workshop
October 2020

Clean Energy Transition Drives High Renewables

EPRI U.S. electric sector carbon reduction models show high wind and solar capacity additions for all 2035 scenarios.

Scenario	Capacity
80% Reduction	561 GW
Net Zero	566 GW
Carbon Free	1,158 GW
100% Renewable	1,766 GW

U.S. Cumulative Capacity Additions 2020 – 2035



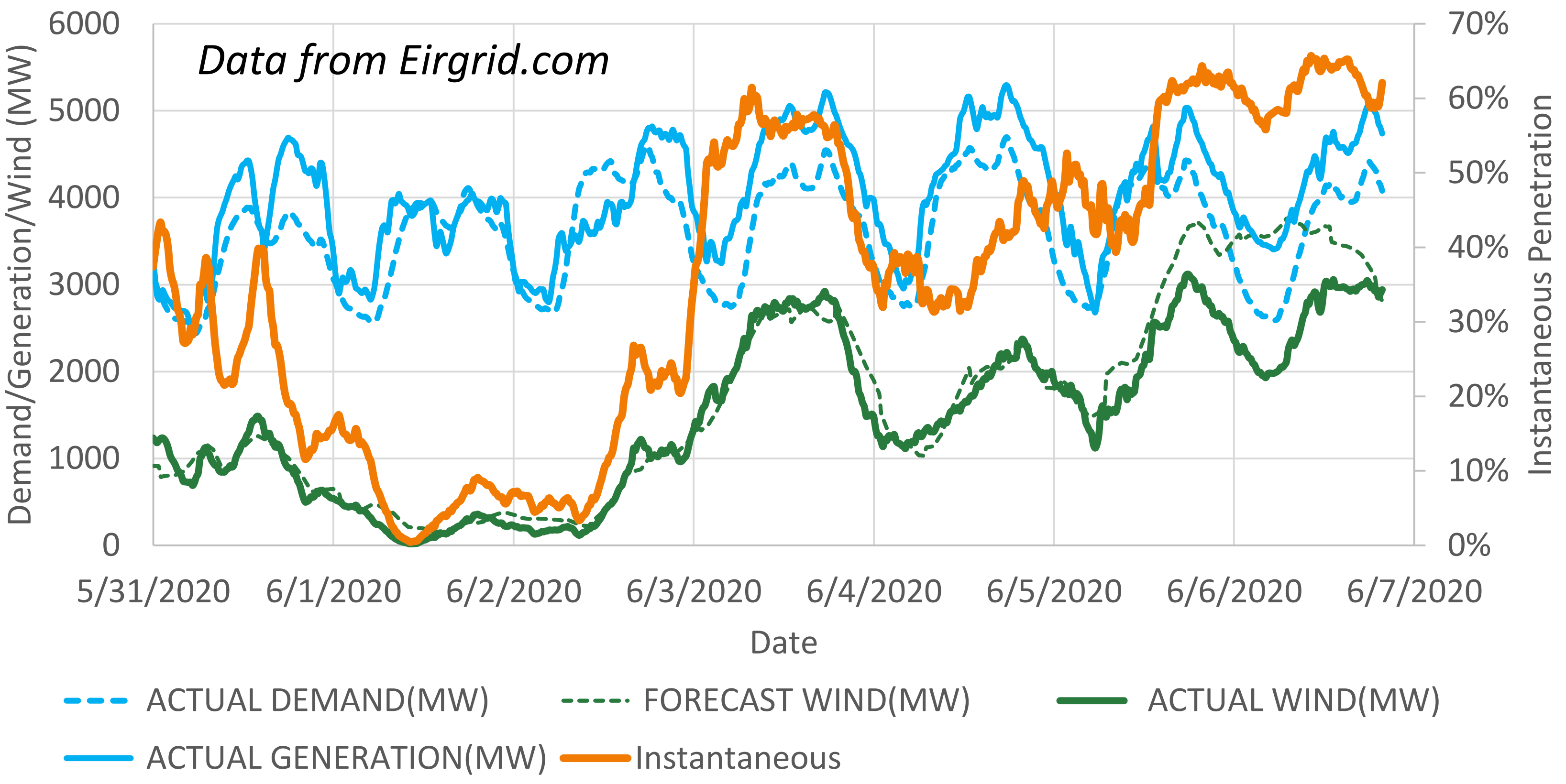
Variability and Uncertainty Considerations

Resource Adequacy
- Planning reserve margin
- Operational flexibility

Transmission Planning
- Which power flow cases?

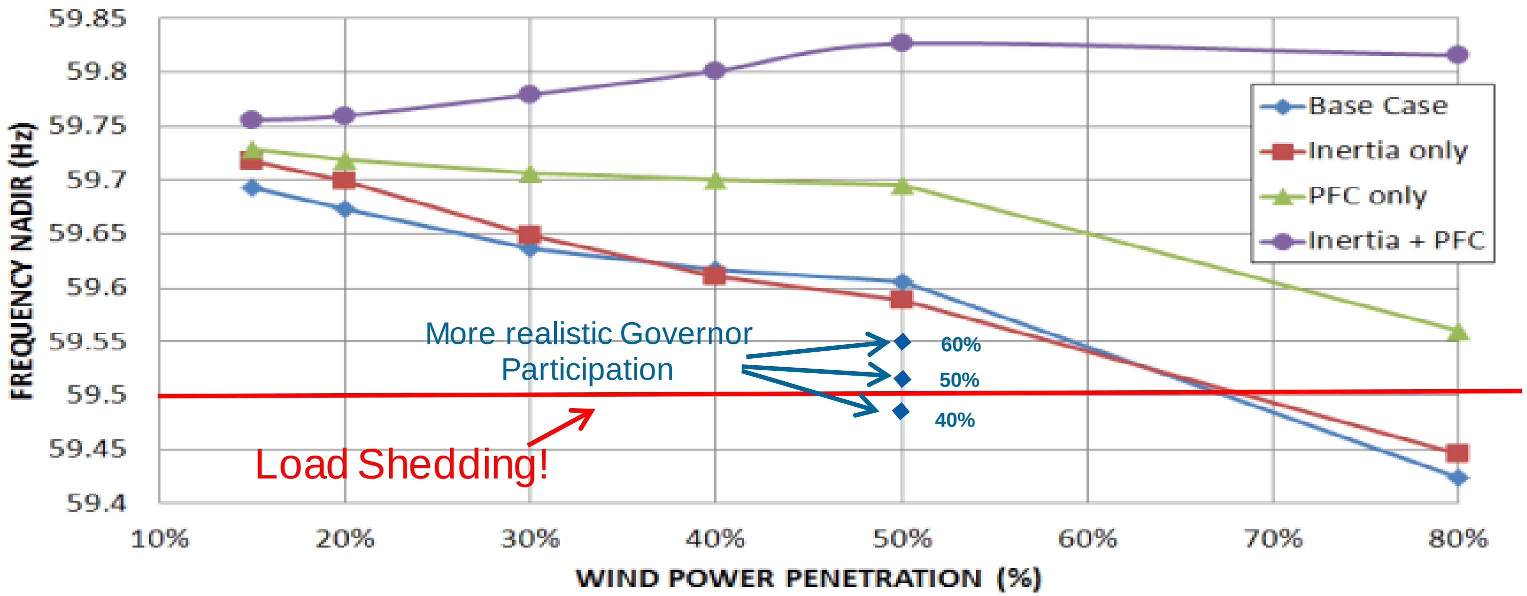
Scheduling & Dispatch
- Higher operating reserve
- Masking of load (DER)

Ops Planning & Real-Time
- Outage scheduling
- System Operating Limits



Reliable integration: Forecasts, control of renewables, optimized reserve requirements, and flexible system

Inverter Interface Resource Considerations



E, Ela et al., *Active Power Control from Wind Power: Bridging the Gaps,* NREL Technical Report, December 2013.

Reliable integration: Validated models, grid forming inverters, distributed control, and grid services from emerging and other resources.

Transmission Reliability

- Displaced inertia/droop
- Inverter controls/capability
- Dynamic behavior
  -- disturbance response
  -- disturbance ride-through

System Protection

- Reduced short circuit
- Different fault response

Transmission Planning

- Validated dynamic models
- Modeling DER in Trans Plan

Operating Reliably at High Renewable Penetrations

Flexible Resources

Operating Reserves

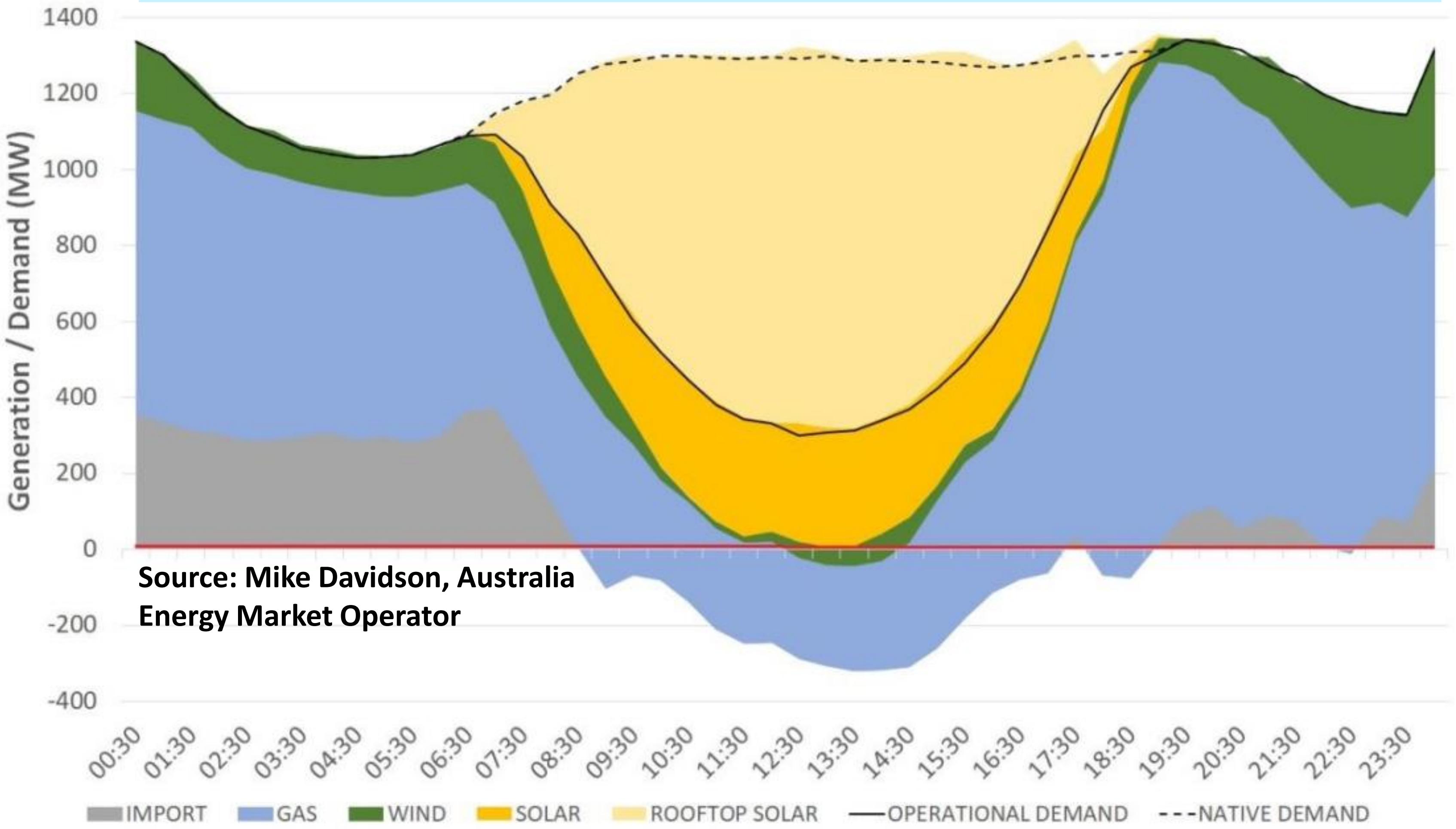
Accurate Forecasting

Transmission Capacity

Grid Reliability Services

Advanced Controls

2020 October 11 South Australia Generation Mix



Today’s max instantaneous scenarios will be normal operation.

Challenges with Penetration Level

Each system is different, but general trends in challenges

Zero to low
- Interconnection requirements
- Validate models

Low (few % annual)
- Integrated forecasting
- Reactive and active control

Medium (low 10s % annual)
- Reserves/flexibility
- Coordination across regions
- 'Duck curve'

High (instantaneous >50%)
- Inertia/frequency support
- Weak grid/stability assessment

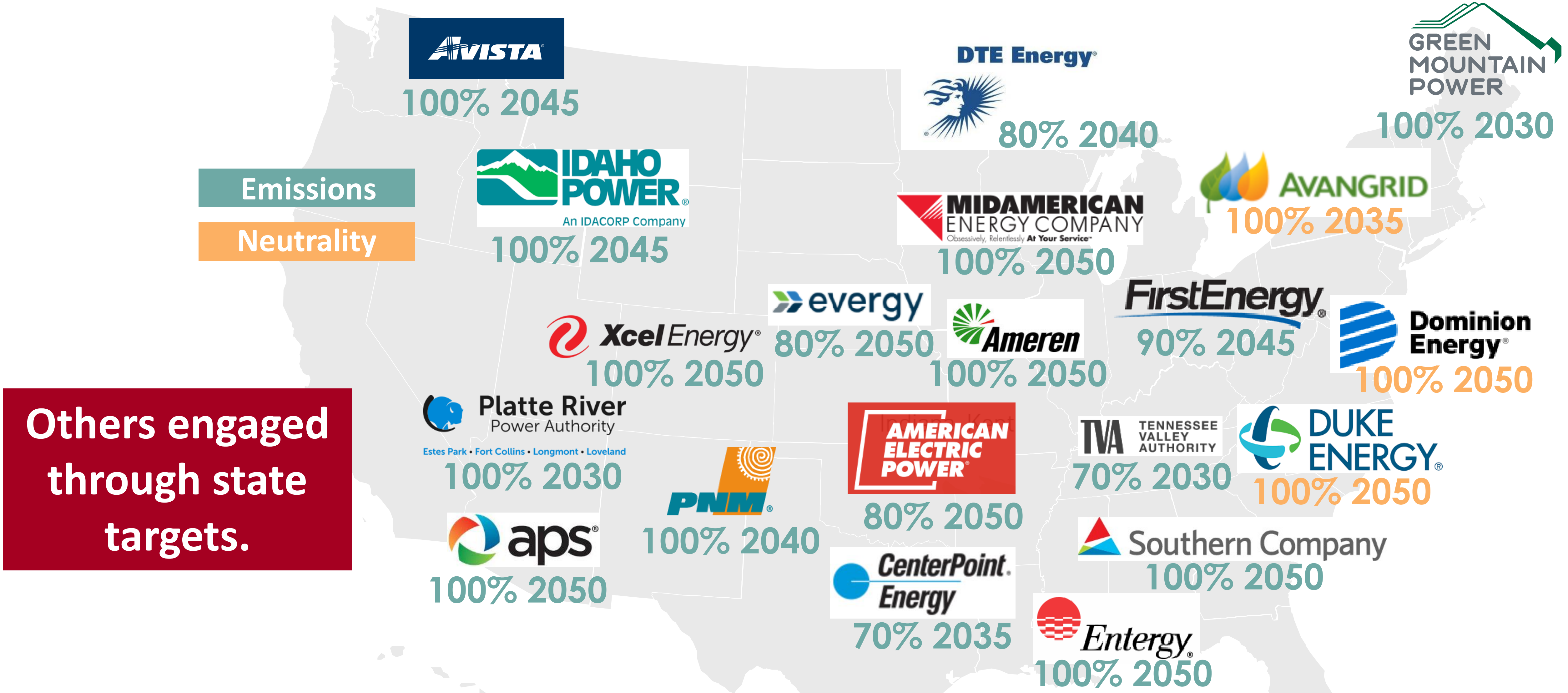
Very high (40%+ annual)
- Seasonal storage
- Grid forming
- Demand side

Need to plan for these issues well before operational

Very few left → Many regions → ERCOT, SPP, Nat. Grid UK, ... → Denmark, Hawaii, South Aus., ...

Together…Shaping the Future of Electricity

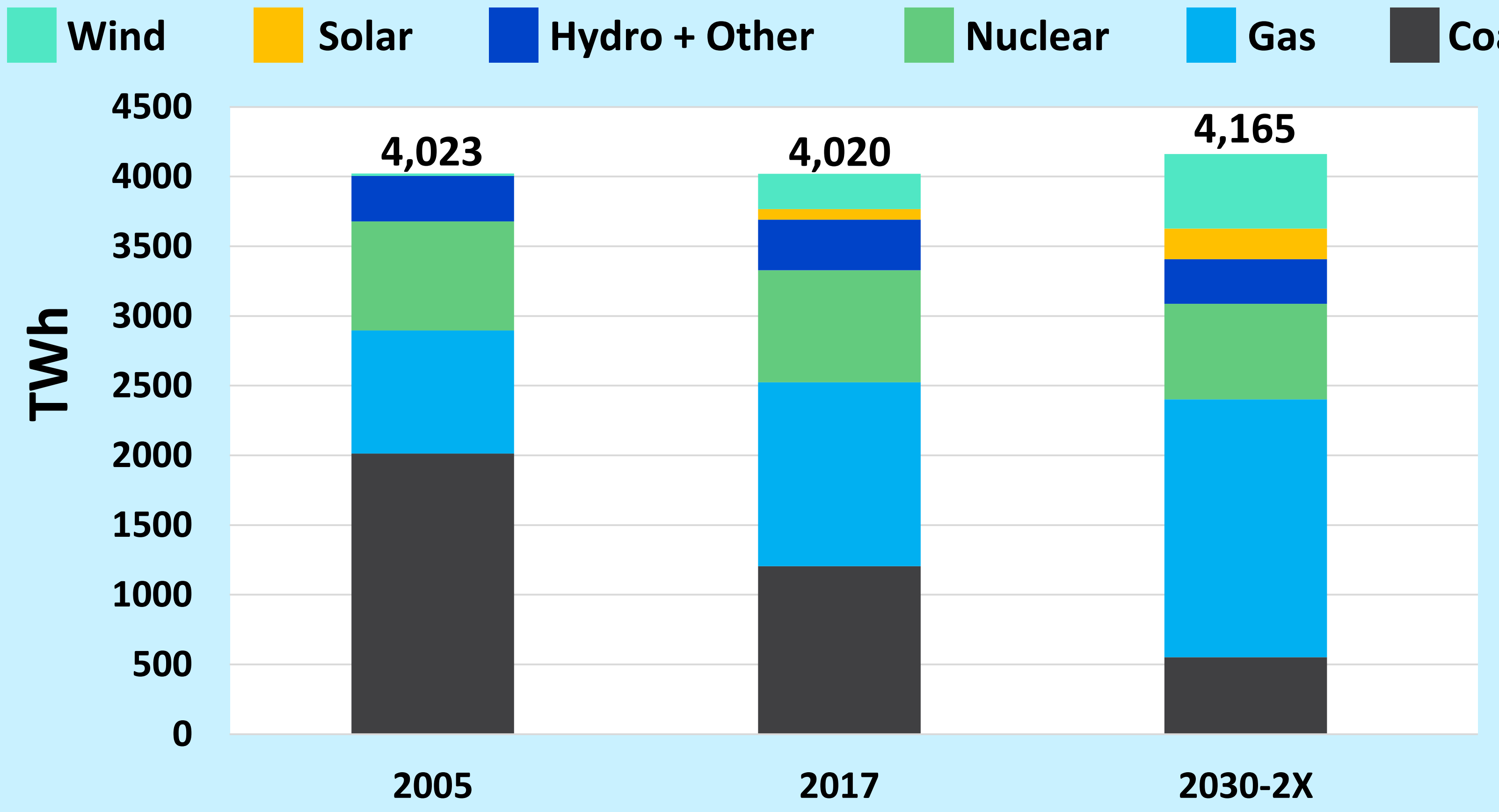
Company-specific carbon reduction commitments



Carbon reduction and climate resiliency key drivers

Electricity Generation Becoming Much Less Carbon-Intensive

Electric Generation Mix Over Time*



Capacity (GW)	2017	2030	2050
Wind	87.6	154.5	221.8
Solar	43.1	129.2	229.5

Carbon Intensity: 0.63 | 0.45 | 0.28

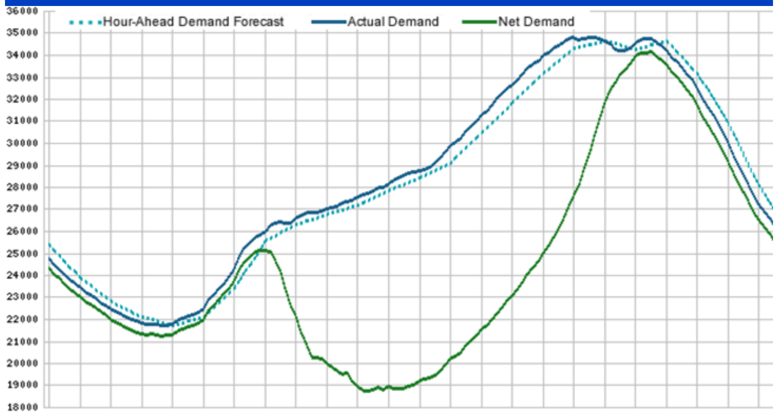
(MT CO_2/MWh)

[1] Historic data from EIA *Monthly Energy Review*, February 2019. Projections from *USREGEN working reference case.*

** Distributed generation included in totals.*

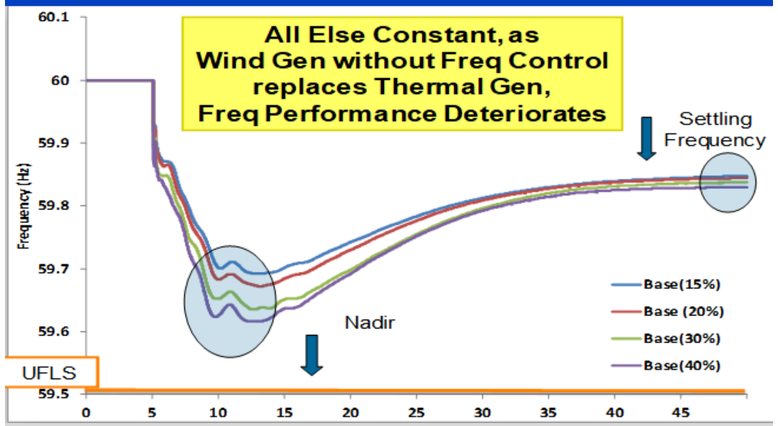
Variable Renewable and Distributed Resource Impacts

Variability/Uncertainty



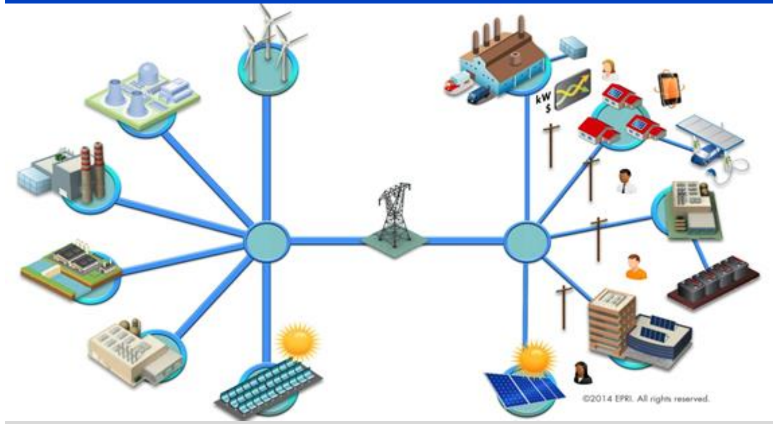
- Output varies over time
- Some correlation between spatially-diverse resources
- Not perfectly predictable or dispatchable
- Zero marginal costs

Inverter-Based



- Power electronic grid interface
- Displaces traditional sources of inertia, short circuit, grid services
- Can be controlled to provide quick responses grid services

Location



- Remote: requires additional transmission and grid strength
- Distributed: can create visibility/control challenges
- Often used to provide multiple services at distribution level

Unique characteristics require new models, methods and tools to reliably integrate.

Operating reliably at high renewable penetrations

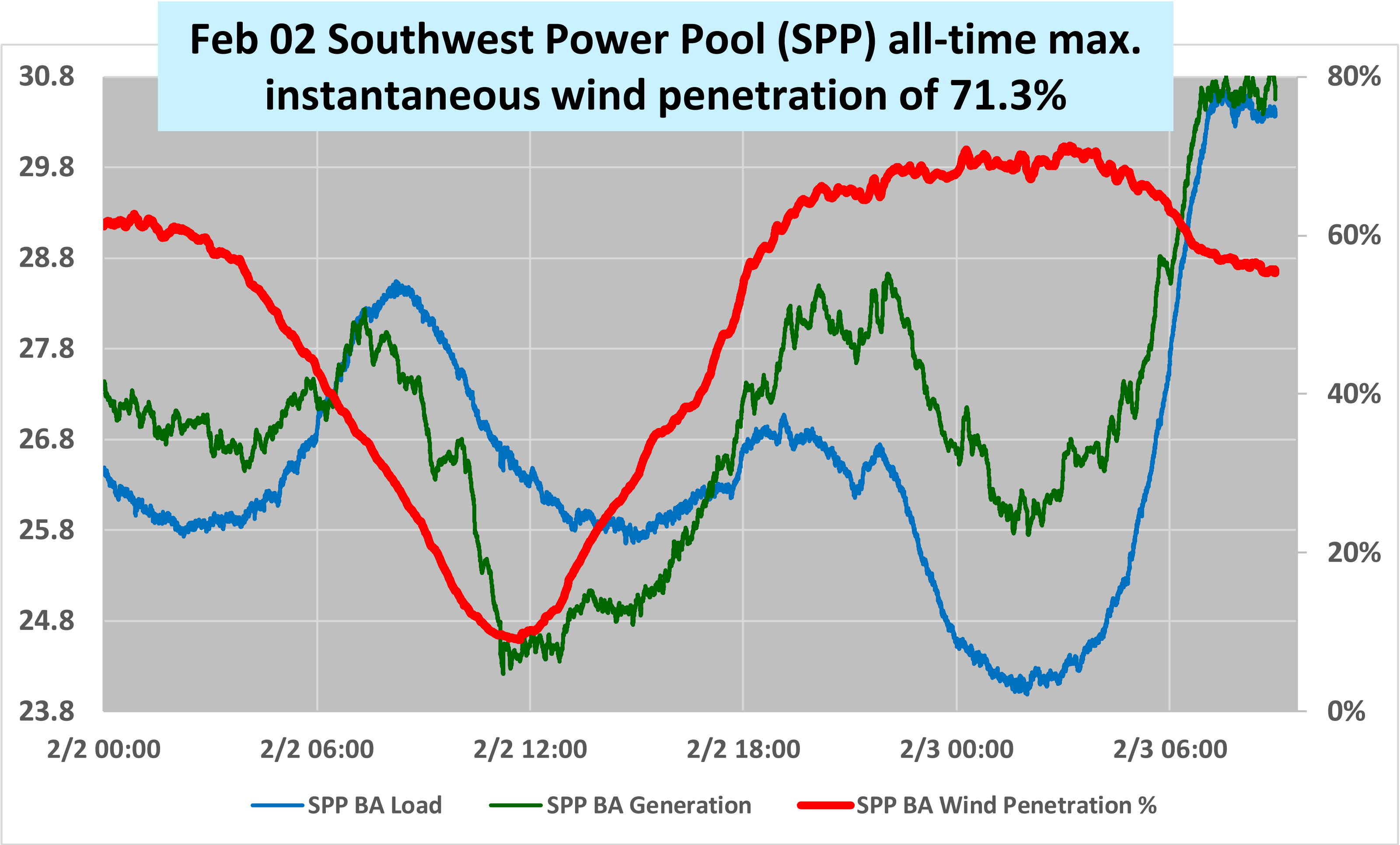
Flexible Resources

Operating Reserves

Accurate Forecasting

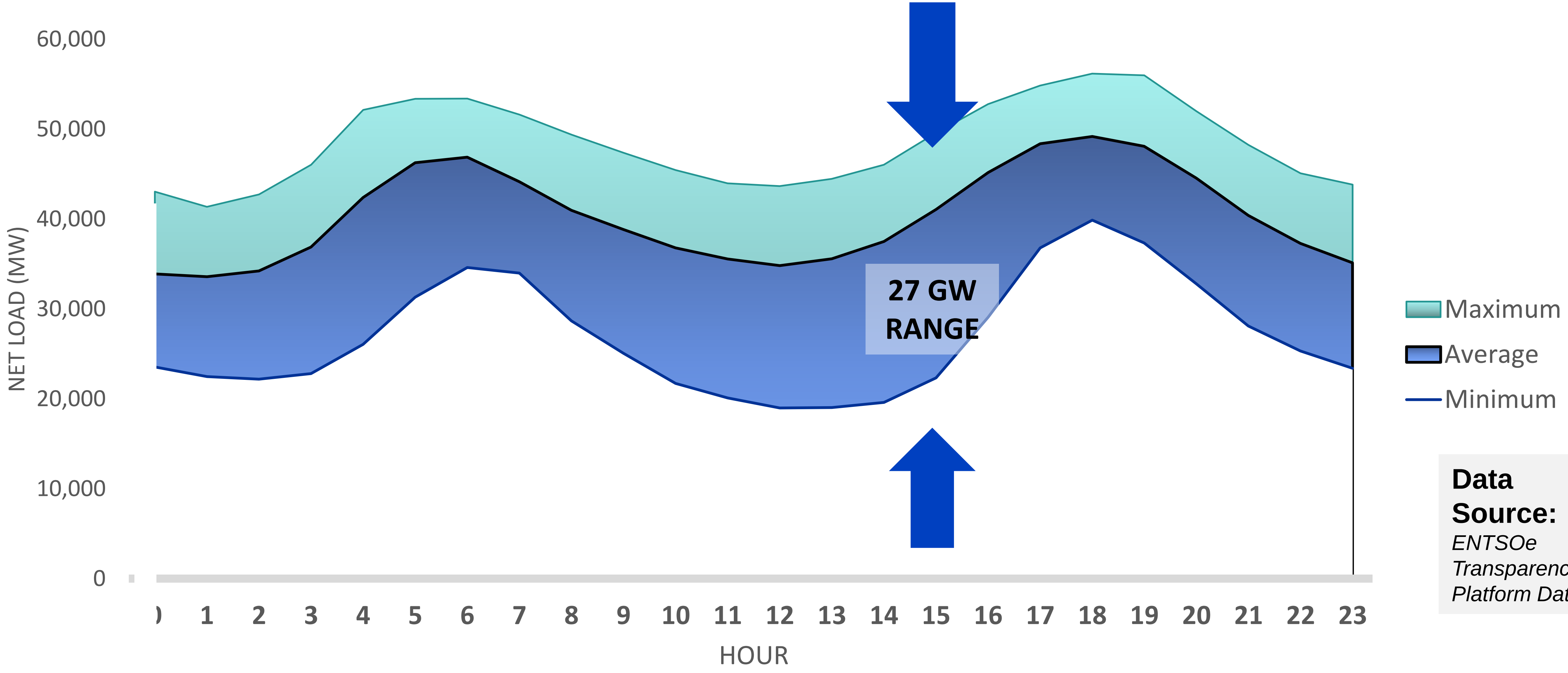
Transmission Capacity

Inverter Stability



Today's max instantaneous scenarios will be normal operation.

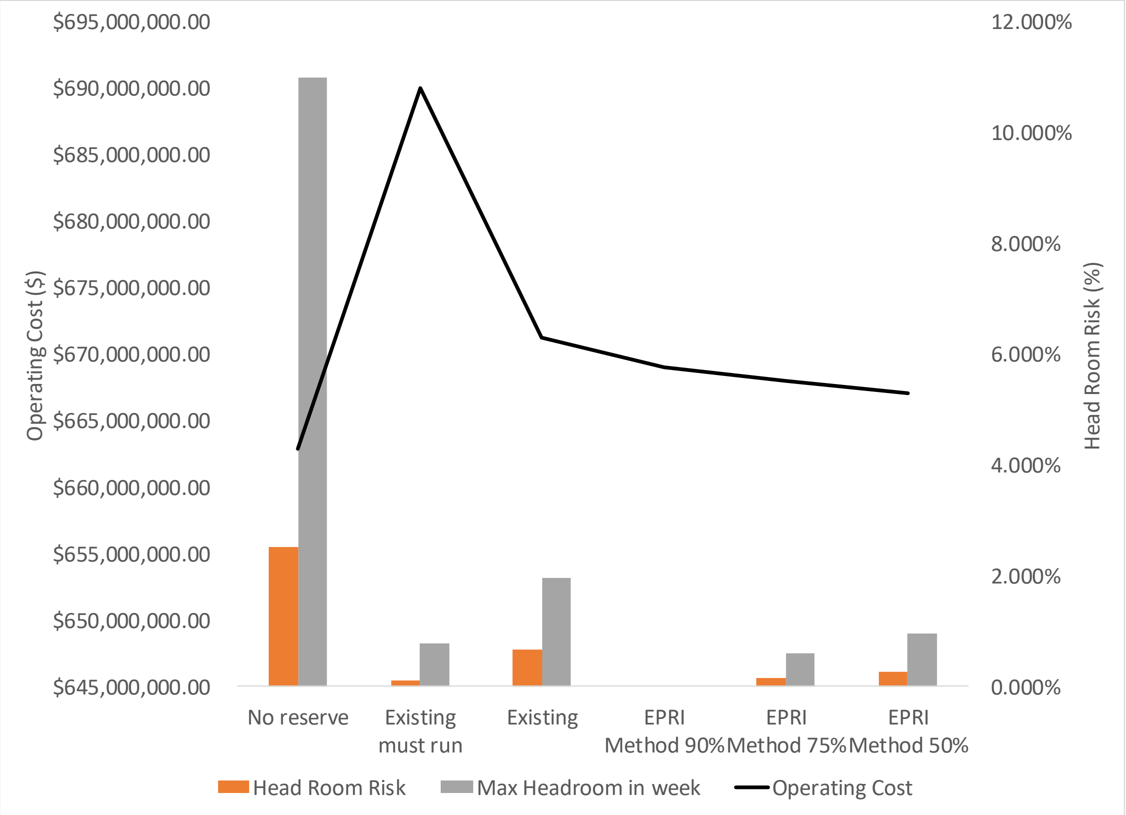
German Hourly Net Load Range – August Workdays, 2019



Data Source:
ENTSOe Transparency Platform Data

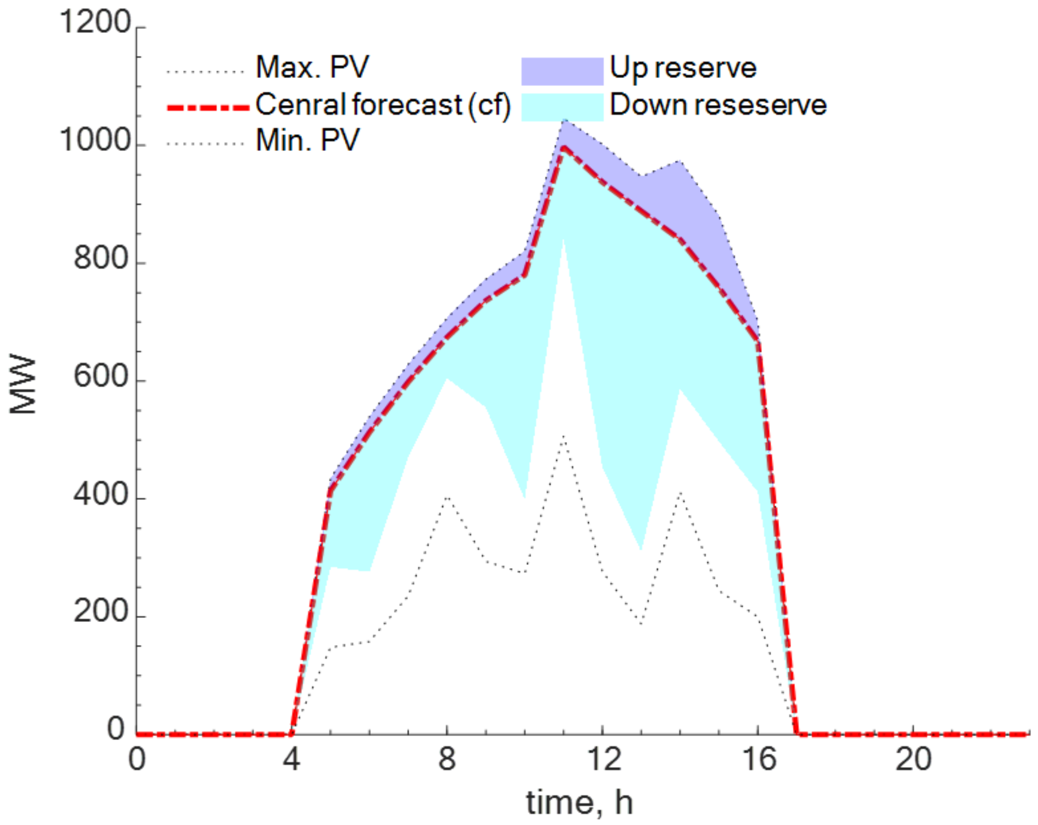
Need methods, models and tools that consider flexibility, risk and nature of resources

Managing Risk in Operations



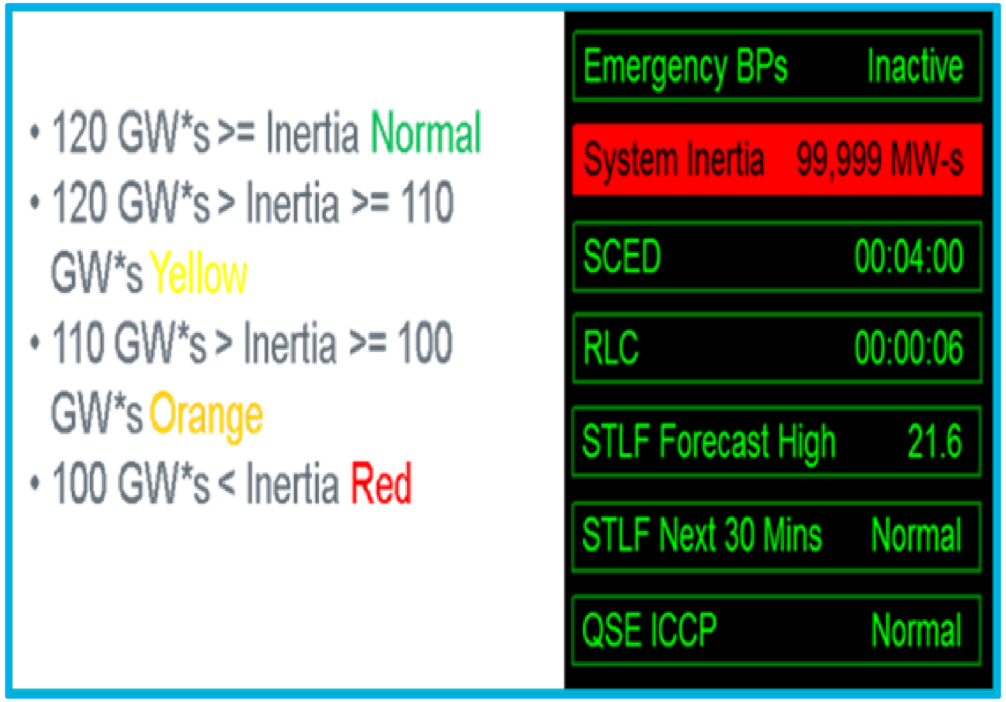
Cost reductions while improving reliability

DOE OPTSUN: Probabilistic Methods

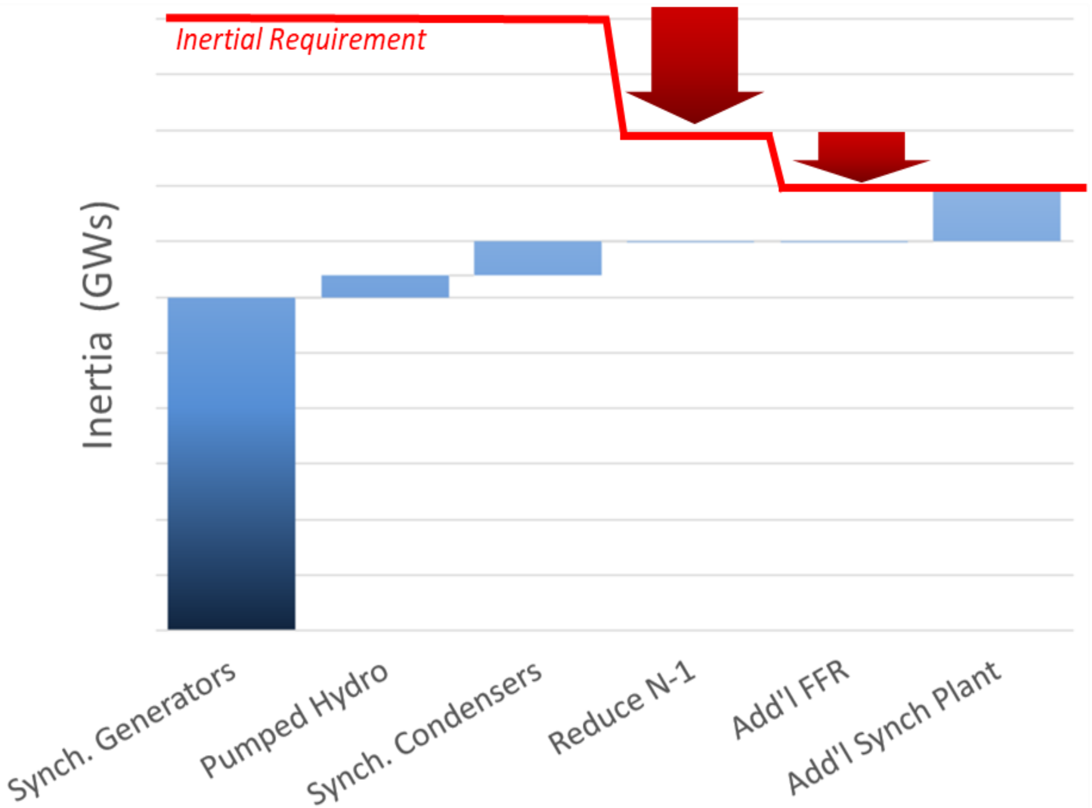


Scheduling and reserves to manage uncertainty in real time

Inertia challenges at interconnection level



ercot



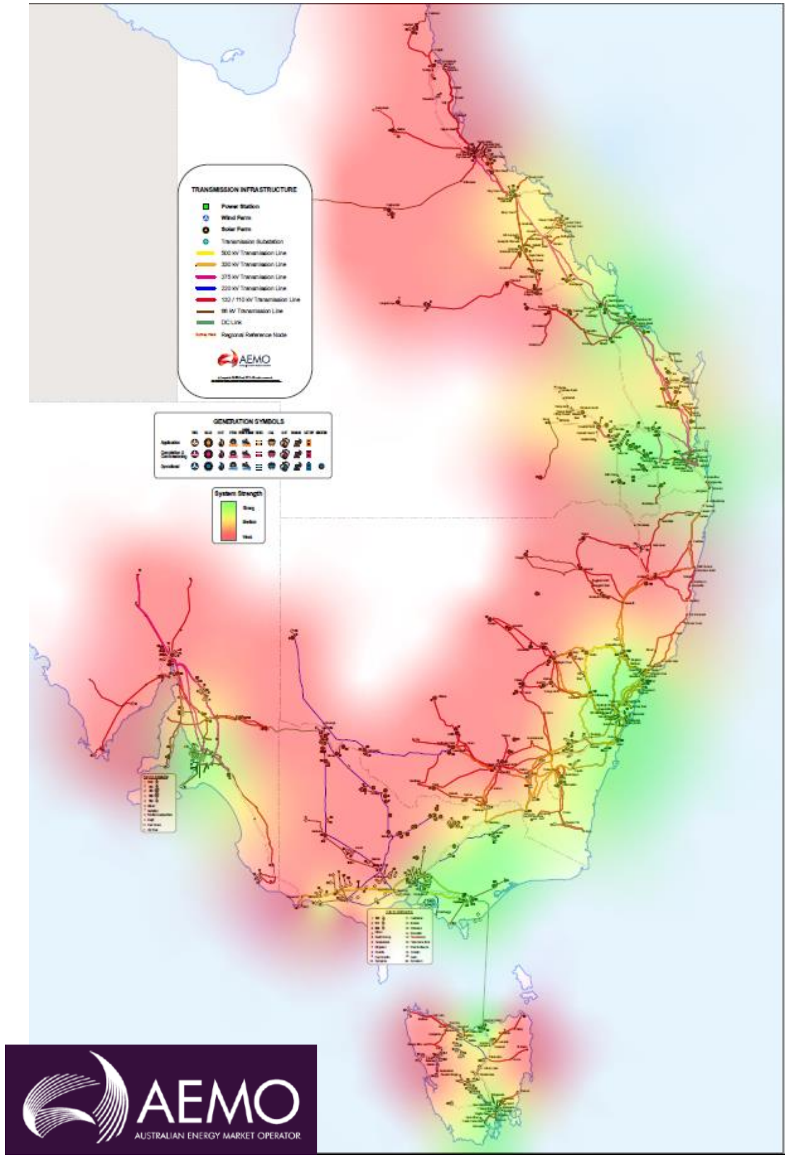
Meeting the Challenges of Declining System Inertia

EPRI Report # 3002015131

New operational paradigms and use of new/existing technology

EPRI ELECTRIC POWER RESEARCH INSTITUTE

System strength at local level



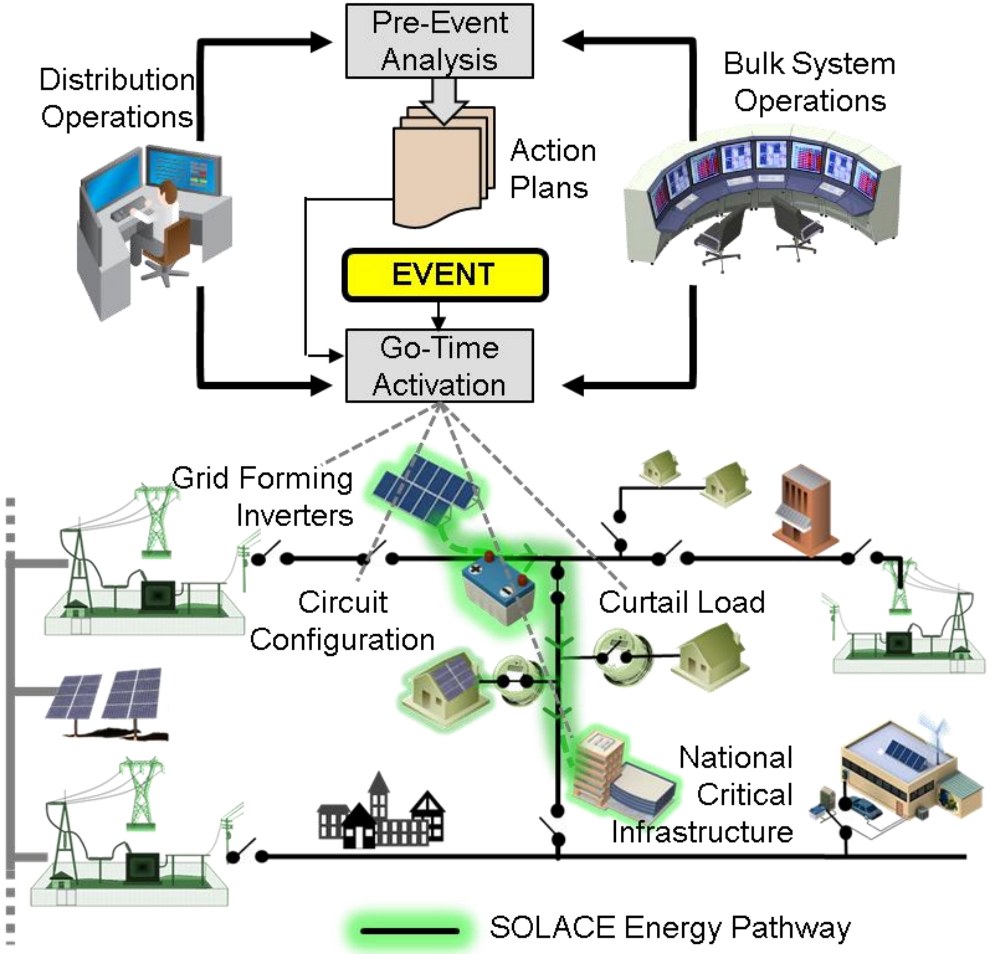
- Synchronous condensers: old solutions, new applications

Source: TasNetworks, Hydro Tasmania

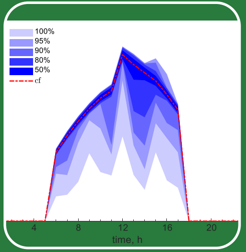
Need models and tools for weak grid issues

Restoration, Resilience and Renewables

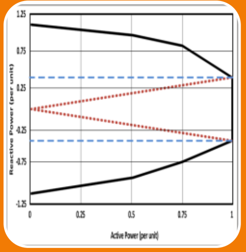
DOE SOLACE Project – Critical Infrastructure



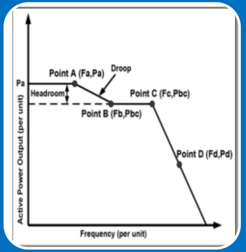
Renewables during Restoration - GREENSTART



Demand and Resource Forecasting

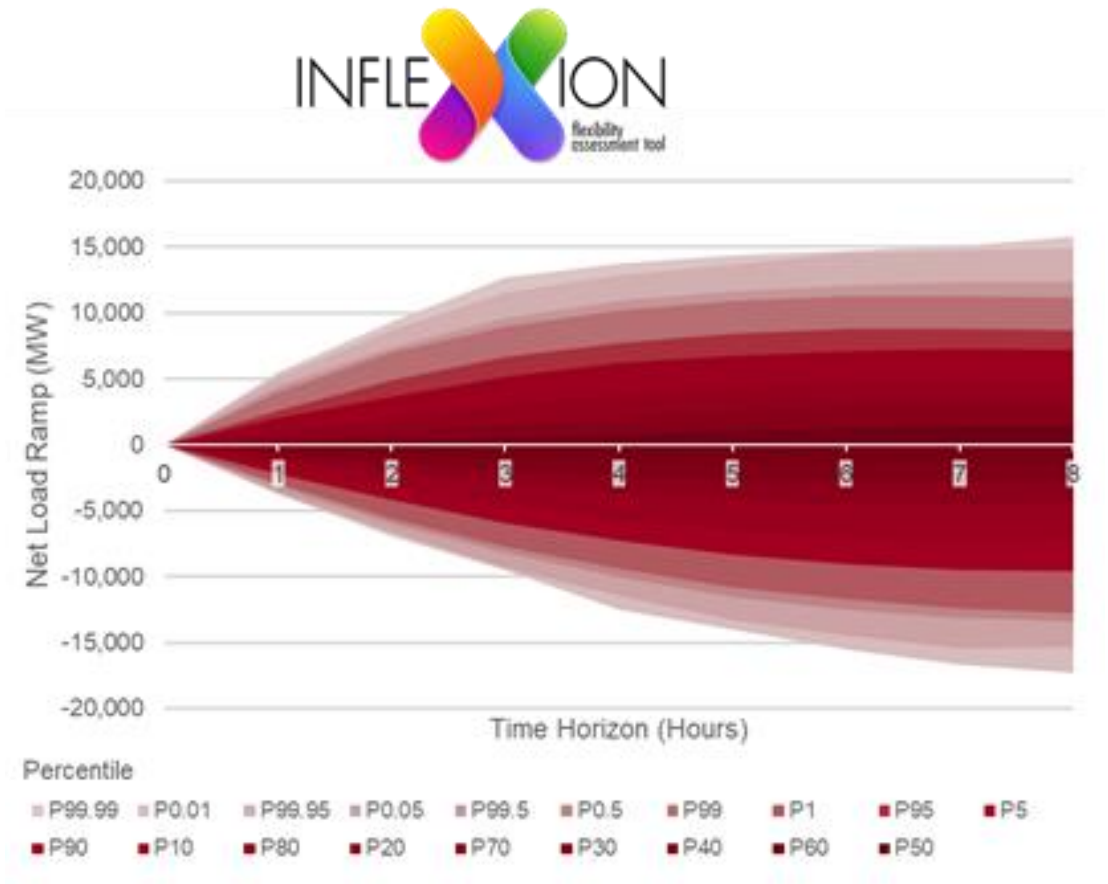


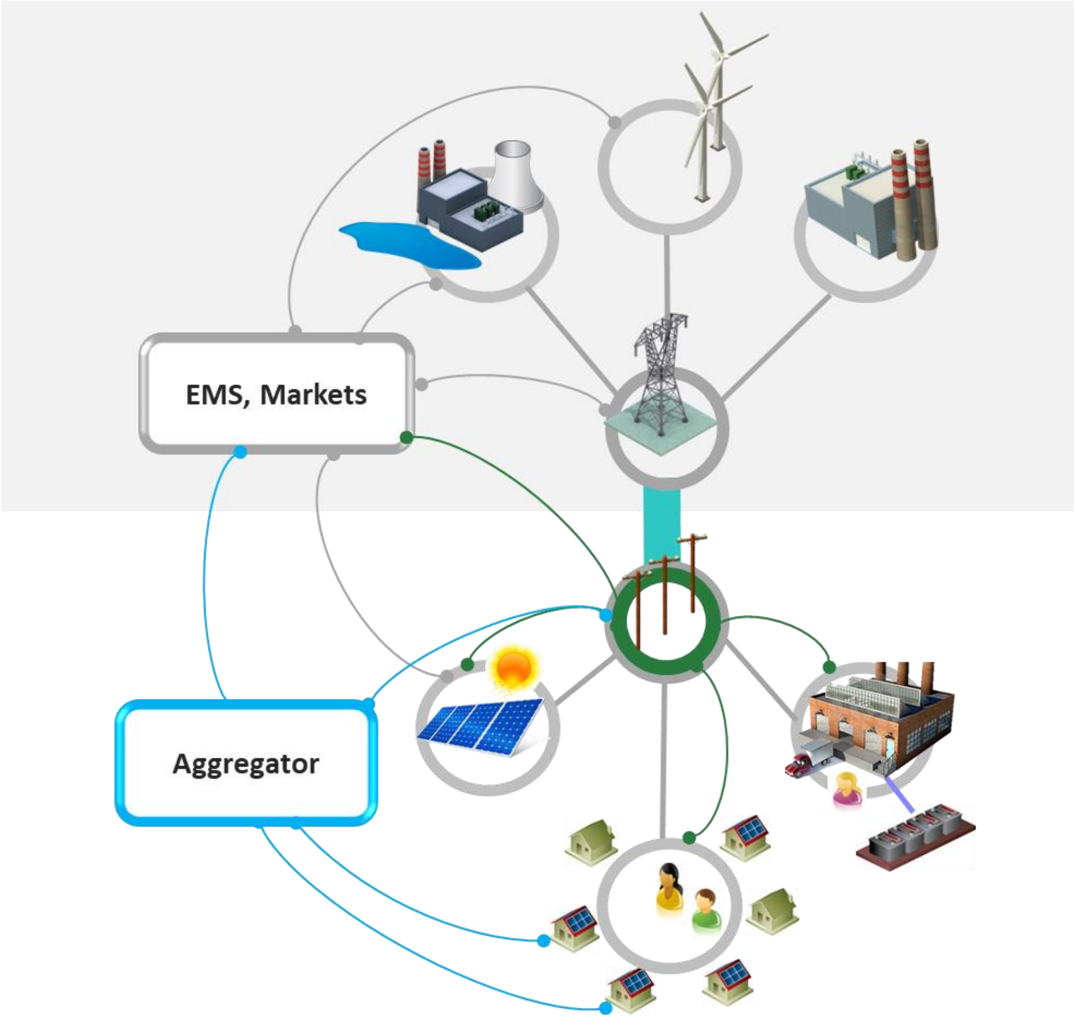
Voltage & Power Control, Inverter & Generator Stability



Protection Sensitivity and Reliability

Flexibility from emerging resources





Need to be able to assess what is needed, and then get it from emerging resources

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Worldwide Systems with Inertia Constraint Characteristics

Recent public reports
EPRI IDs: 3002015131, 3002015132
https://youtu.be/ZCa2LHxq9C8

ERCOT

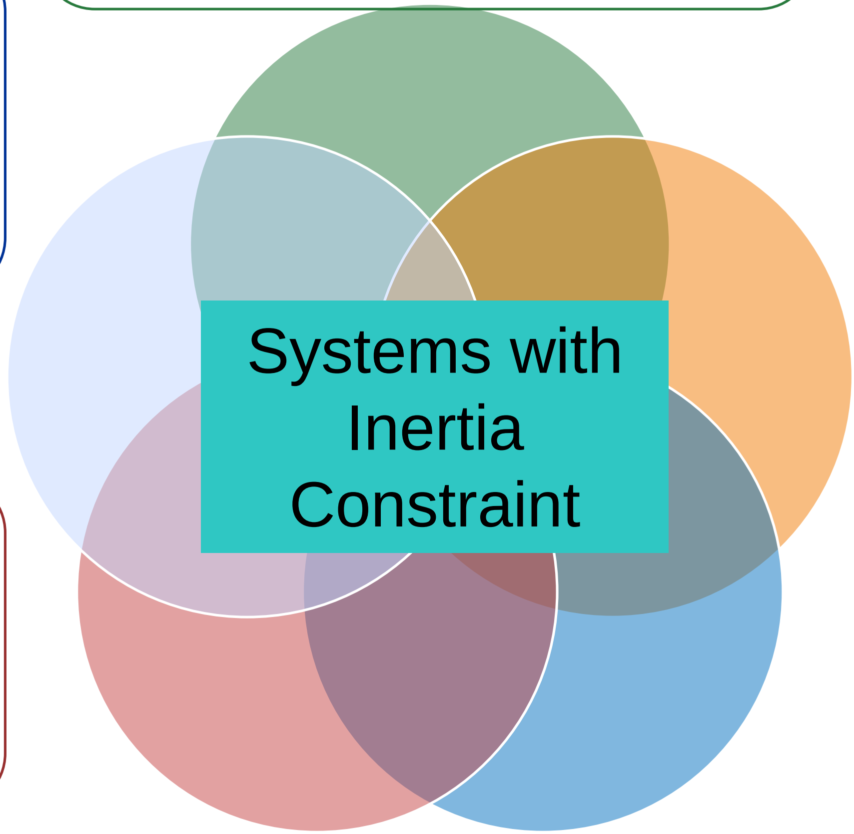
- Inertia floor of 100 GWs
- Online monitoring
- Proposed ancillary service market redesign, SIR, FFR, PFR

NORDIC

- Inertia floor of 120 GWs
- Online monitoring
- Redispatch design contingency nuclear unit for inertia constraint

Ireland

- Inertia floor of 23 GWs
- Minimum unit constraint
- RoCoF upgrade project to 1 Hz/s
- Ancillary services market redesign with SIR
- Auction-based market for SIR



Australia

- Inertia floor of 6.2 GWs
- Minimum unit constraint
- Online monitoring, inertia, and stability

NG UK

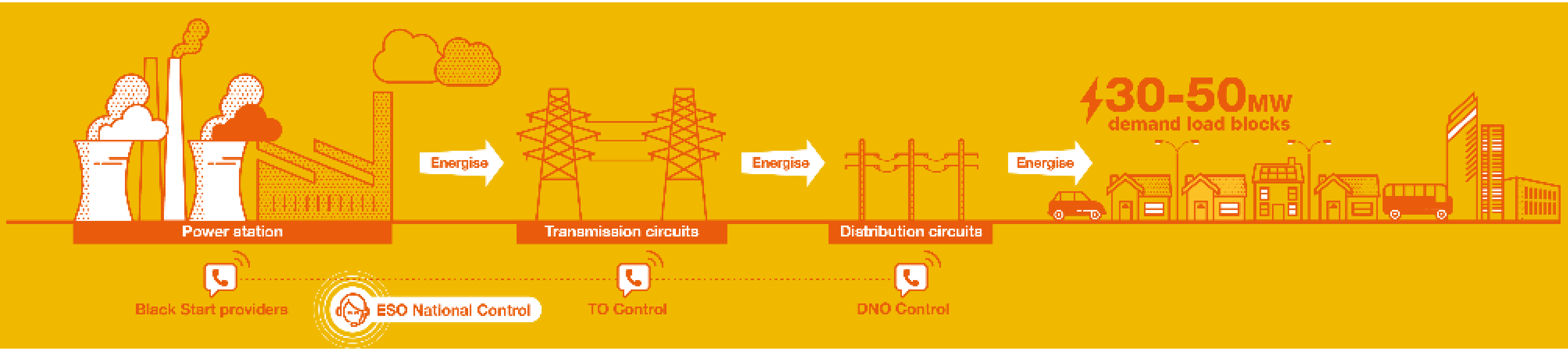
- Inertia floor of 135 GWs
- RoCoF upgrade project to 1 Hz/s
- Ancillary service market redesign with EFR similar to FFR (storage)

Credit to:

Roisin Quinn
National Grid ESO

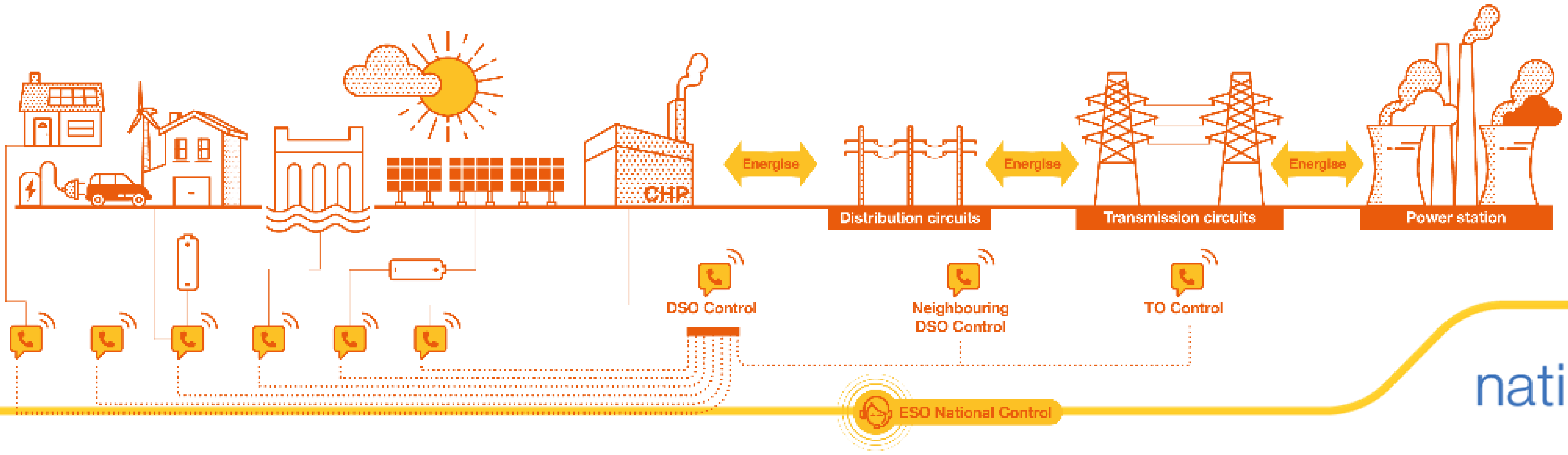
nationalgridESO

Distributed ReStart



Conventional Black Start

Distributed ReStart will enable the transition by engaging DERs in a ‘first in world’ bottom up restoration service



Future Black Start

nationalgridESO

Distributed ReStart looks to deliver against the success criteria below:

Reduced costs to consumers of up to £115M by 2050

Savings of up to 810,000 Tonnes CO2

energy.

with **renewable**

to prove **it's possible**

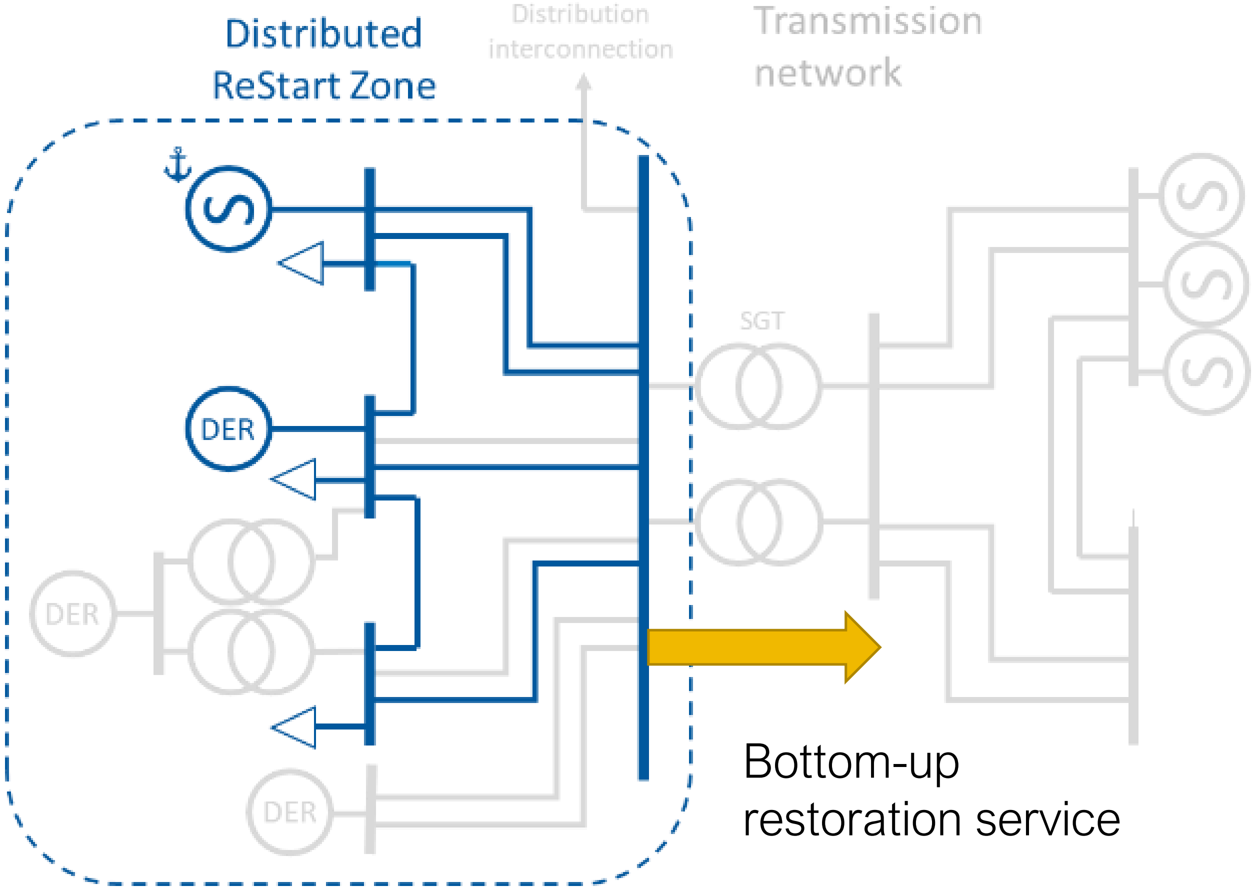
approach to **black start,**

This project uses a **bottom up**

We have already achieved lots through the project.

Across the project we have:

- Carried out extensive power system studies to develop restoration strategies
- Developed case studies ready for live trials
- Scoped the telecommunication change requirements
- Developed an organisational structure and control procedure
- Designed a preferred commercial structure



- Technical and commercial design stage reports available at: https://www.nationalgrideso.com/future-energy/projects/distributed-restart

nationalgridESO

We are working on lots of other exciting projects to enable zero carbon operation.

- New Balancing services
- Pathfinder projects – voltage, stability, thermal constraints
- Accelerated loss of mains
- Power Potential
- Wider access to the Balancing Mechanism
- Launch of Dynamic Containment as part of a suite of frequency response products
- ENA Open Networks project

Thank You

We are passionate about driving the energy transition and helping GB achieve it’s net-zero target.

We are keen to work closely with others in the industry so that we can continue to deliver clean, green, reliable and affordable electricity to all.

www.nationalgrideso.com

Barry O’Connell, Australian Energy Market Operator

Click link below to access video presentation:

https://www.youtube.com/watch?v=yX_XKzc8p-M&feature=youtu.be

From Cyber-Security to the Cyber-Physical Resilience of the Electric Power Grid: An Agenda Forward

Amro M. Farid
Associate Professor of Engineering

Thayer School of Engineering at Dartmouth

LIINES LABORATORY FOR INTELLIGENT INTEGRATED NETWORKS OF ENGINEERING SYSTEMS
EMPOWERING YOUR NETWORK

http://engineering.dartmouth.edu/liines

Invited Presentation
The Seventh Annual EPRI-IEA Challenges in Energy Decarbonisation Expert Workshop
Paris, FR / Virtual
October 29, 2020

Presentation Goal

To give an even-handed "woods-from-the-trees" perspective on the cyber-physical resilience of the electric power grid despite …

- **… 12 minutes**
- **… A very active & noisy space**
- **… Prone to sensationalism**

Cyber-security → Cyber-Physical Resilience
w/ innovations in grid technologies, markets, and policy

1. Famous Cyber-Attacks on the Electric Power Grid

How 30 Lines of Code Blew Up a 27-Ton Generator

A secret experiment in 2007 proved that hackers could devastate power grid equipment beyond repair—with a file no bigger than a gif.

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

In an excerpt from her new book, "Countdown to Zero Day," WIRED's Kim Zetter describes the dark path the world's first digital weapon took to reach its target in Iran.

'Crash Override': The Malware That Took Down a Power Grid

In Ukraine, researchers have found the first real-world malware that attacks physical infrastructure since Stuxnet.

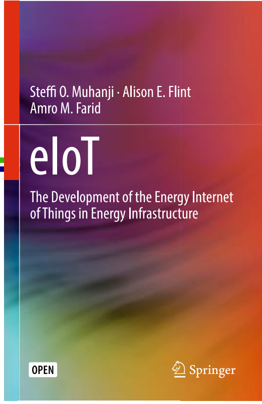
The Aurora Generator Test

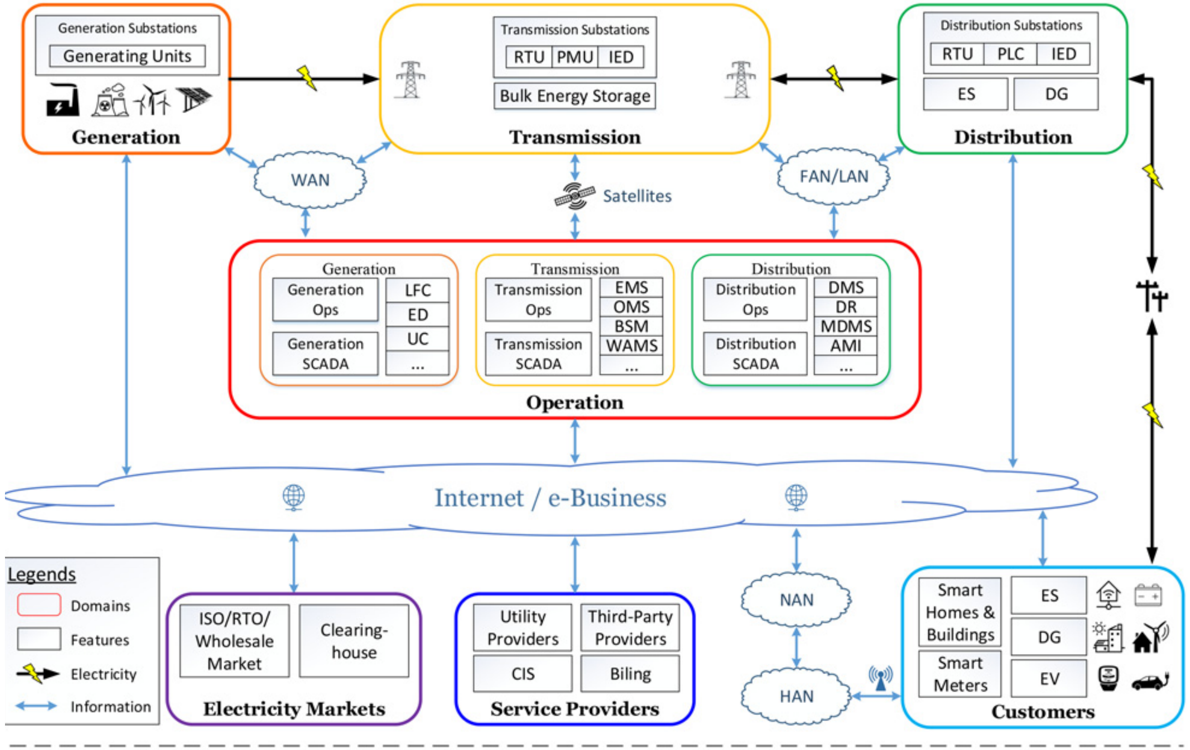
Stuxnet's Centrifuges

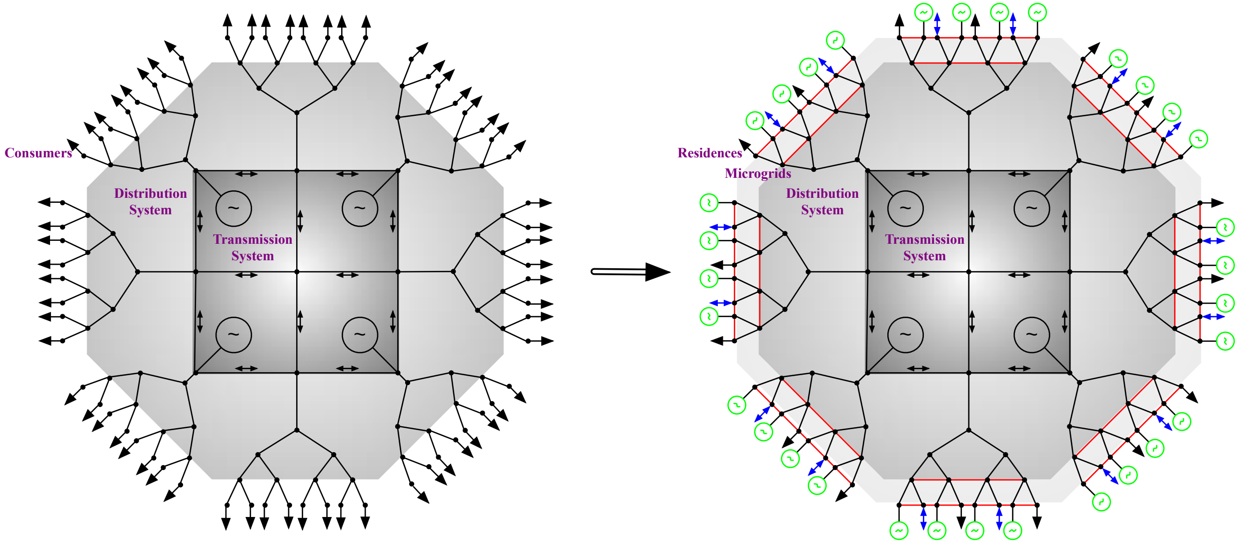
Crash Override's Substation

The Anecdotal Evidence Indicates the Severity of the Problem.

2. The Grid's Daunting & Ever-Growing Attack Surface

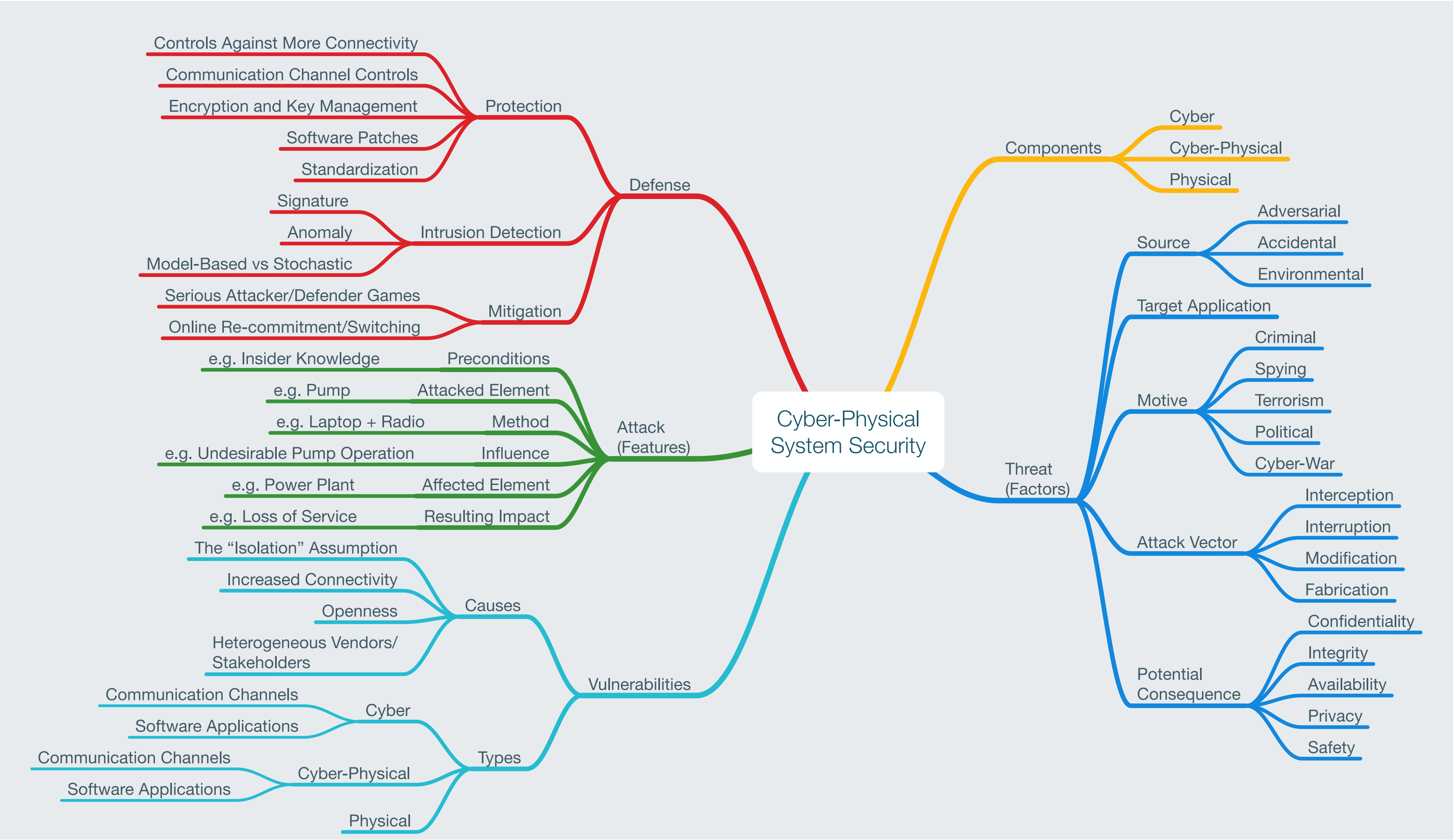






Anecdotal Evidence of Cyber-Attacks Understate the Problem.

3. Coping with Complexity: Cyber-Security Frameworks



Desperate Need to Apply Systems Thinking to Manage Complexity.   …But can we do it all?

4. Shotgun Test: Convergence of Cyber & Physical Security

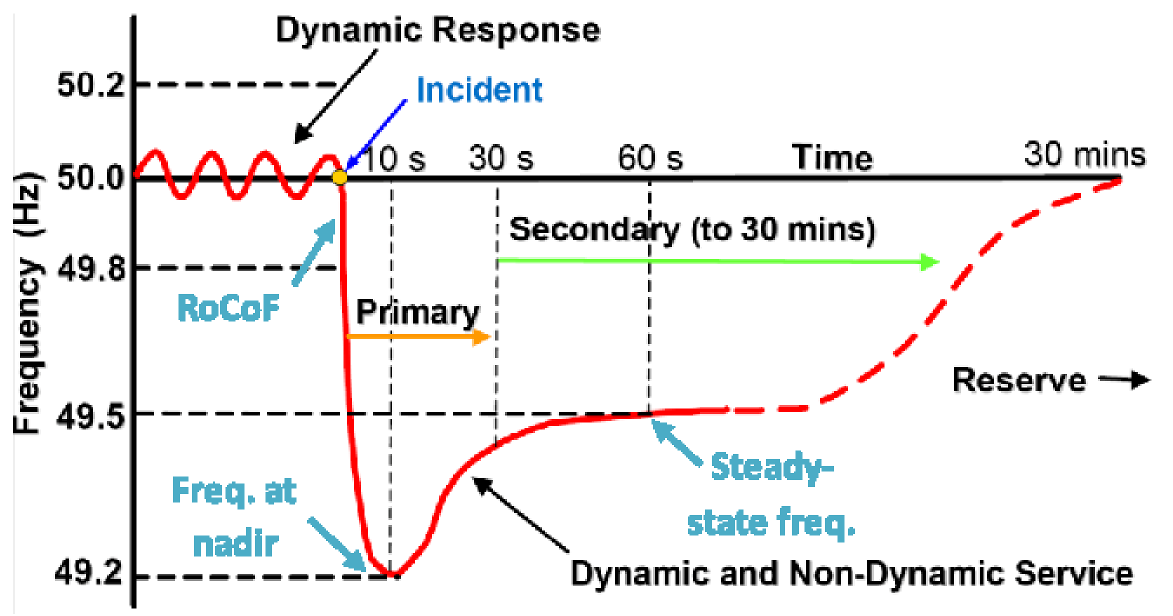
Power Systems Engineer (Skeptical)	Cyber-Security Scientist (Enthusiastic)
Shotgun Test: "But is all of this any worse than a disgruntled customer one day getting their shotgun and shooting at the local substation?"	**A:** "The cyber-attacker can take out the substation without detection or being apprehended."
N-1 Contingency Analysis Test: "But is all of this worse than me losing my 1.5 GW Nuclear Generator & 2GW Tie Line as my largest contingencies? I can already handle that!"	**A:** **"**The cyber-attacker doesn't need to take out the largest contingency. They can take out multiple coordinated facilities simultaneously. You need N-X Contingency Analysis."
Stability Test: "So what does this cyber-security stuff mean for frequency, voltage, and stability analyses?"	**A:** "Umm… grid stability?"
Reliability Test: "So what does this mean for my reliability measures LOLE, LOLP, SAIDI, SAIFI?"	**A:** "It's pretty difficult to quantify these measures when new threats are being devised all the time and their probabilities are unknown".
Market Stability Test: "So what does this mean for the stability of the grid's markets and services?"	**A:** "They're a target. Some market designs are structurally better than others. The threat severity is still unknown."

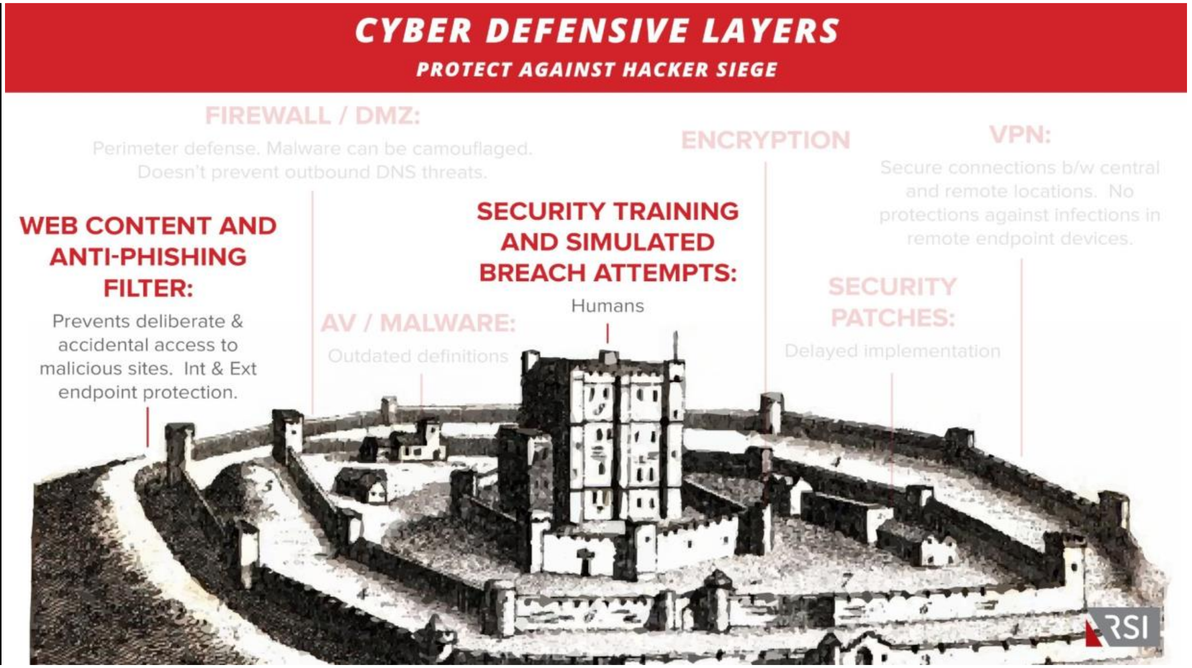
Cyber-Physical Convergence → Integrated Threat Severity Threat Assessment

5. Accepting Disruption: Resilient Survival & Response

A "Resilience Mindset" is integral to both power systems engineering and cyber-security practice.

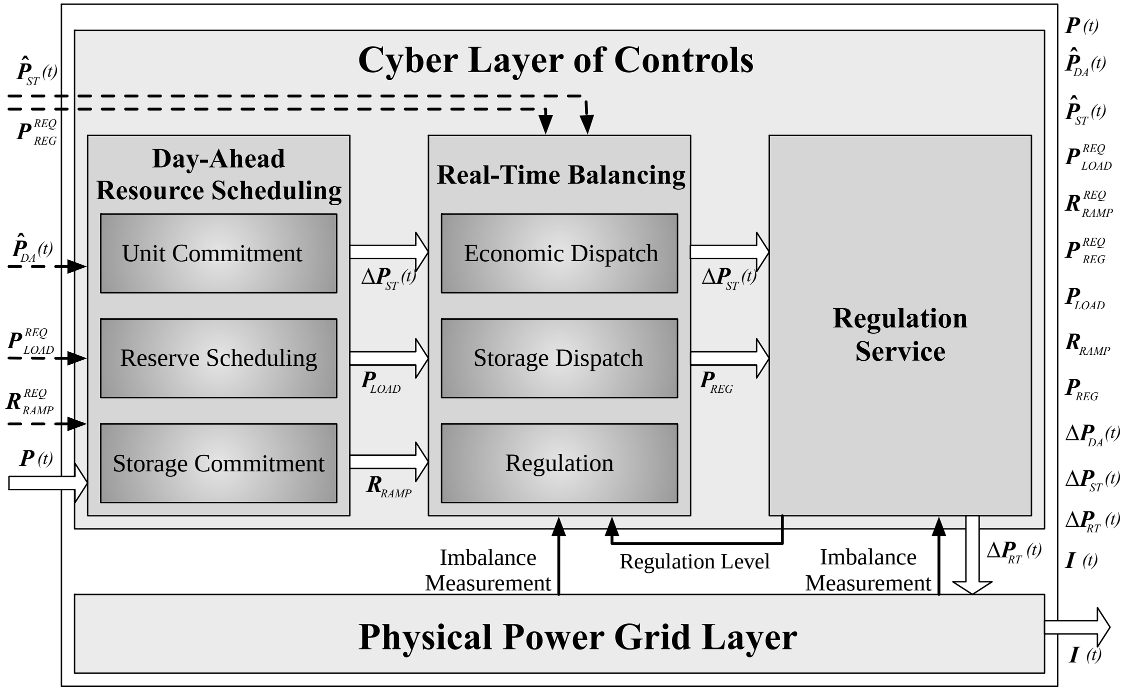
Power Systems Engineer	Cyber-Security Scientist



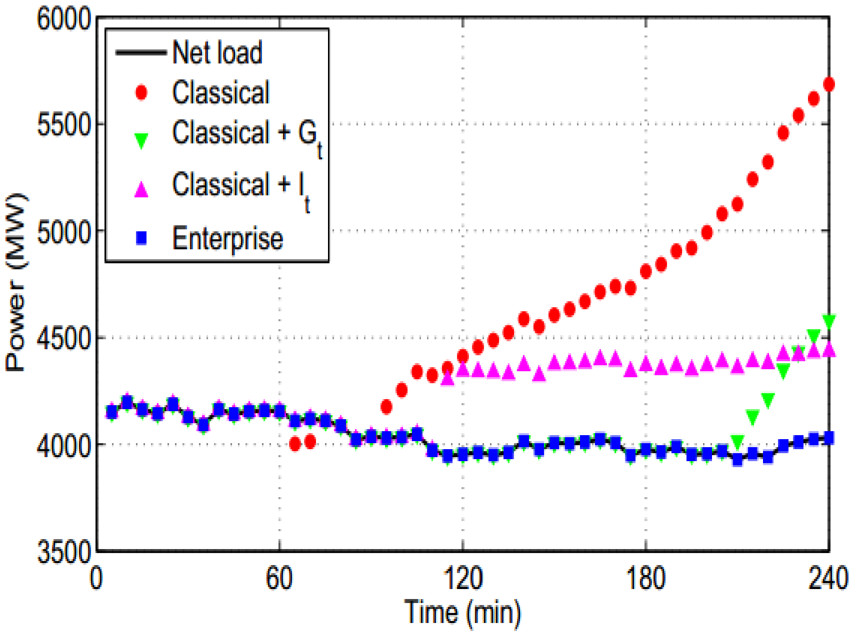


Blackouts Happen. Components will Fail. What matters is how we survive them, respond & learn.

6. The Need for Dynamic & Holistic Approaches: An Electric Power Enterprise Control System Example



- $P(t)$ - Actual net load;
- $\hat{P}_{DA}(t)$ - Net load day-ahead forecast;
- $\hat{P}_{ST}(t)$ - Net load short-term forecast;
- P^{REQ}_{LOAD} - Load following reserve requirement;
- R^{REQ}_{RAMP} - Ramping reserve requirement;
- P^{REQ}_{REG} - Regulation reserve requirement;
- P_{LOAD} - Actually scheduled load following reserves;
- R_{RAMP} - Actually scheduled ramping reserves;
- P_{REG} - Actually scheduled regulation reserves;
- $\Delta P_{DA}(t)$ - Imbalances at the day-ahead scheduling output;
- $\Delta P_{ST}(t)$ - Imbalances at the real-time balancing output;
- $\Delta P_{RT}(t)$ - Imbalances at the regulation service output;
- $I(t)$ - Residual imbalance at the system output;



∴ **EPECS Simulation has been used to study techno-economic system performance in the presence of variable renewable energy resources.**

∴ **Small changes in the information flow between power systems markets and controllers can lead to system-wide instabilities.**

Conclusion: Take Home Points

1. The electric power grid has already suffered debilitating cyber-attacks from highly sophisticated adversaries, and the severity and sophistication is only expected to grow.
2. As the largest machine ever built, the electric power grid presents a daunting ever-growing “attack surface” of cyber and cyber-physical interfaces.
3. In order to cope with the unprecedented complexity, cyber-security frameworks composed of taxonomies of components, threats, vulnerabilities, attacks, and defenses are being developed.
4. The cyber-security paradigm of security for every cyber-interface must converge with a practical physical security paradigm.
5. Blackouts Happen: How we survive them, respond & learn is what is important.
6. Much like VRE integration, dynamic and holistic approaches are necessary to objectively assess severity and design mitigating solutions.

Cyber-security → Cyber-Physical Resilience

w/ innovations in grid technologies, markets, and policy

References

- [1] W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” Computer networks, vol. 57, no. 5, pp. 1344–1371, 2013.
- [2] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid and smart home security: Issues, challenges and countermeasures,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933– 1954, 2014.
- [3] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-physical systems security—a survey,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2017.
- [4] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, “A survey of cyber security management in industrial control systems,” International journal of critical infrastructure protection, vol. 9, pp. 52–80, 2015.
- [5] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, “False data injection on state estimation in power systems—attacks, impacts, and defense: A survey,” IEEE Transactions on Industrial Informatics, vol. 13, no. 2, pp. 411–423, 2016.
- [6] H. He and J. Yan, “Cyber-physical attacks and defences in the smart grid: a survey,” IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 13–27, 2016.
- [7] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, “Survey of security advances in smart grid: A data driven approach,” IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 397–422, 2017.
- [8] M. R. Asghar, G. D´an, D. Miorandi, and I. Chlamtac, “Smart meter data privacy: A survey,” IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2820–2835, 2017.
- [9] R. Atat, L. Liu, J. Wu, G. Li, C. Ye, and Y. Yang, “Big data meet cyber-physical systems: A panoramic survey,” IEEE Access, vol. 6, pp. 73603–73636, 2018.
- [10] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, “Cyber-security in smart grid: Survey and challenges,” Computers & Electrical Engineering, vol. 67, pp. 469–482, 2018.
- [11] D. B. Rawat and C. Bajracharya, “Cyber security for smart grid systems: Status, challenges and perspectives,” in SoutheastCon 2015, pp. 1–6, IEEE, 2015.
- [12] A. Abedi, L. Gaudard, and F. Romerio, “Review of major approaches to analyze vulnerability in power system,” Reliability Engineering & System Safety, vol. 183, pp. 153–172, 2019.
- [13] U. P. D. Ani, H. He, and A. Tiwari, “Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective,” Journal of Cyber Security Technology, vol. 1, no. 1, pp. 32–74, 2017.
- [14] M. A. Ferrag, L. A. Maglaras, H. Janicke, and J. Jiang, “A survey on privacy-preserving schemes for smart grid communications,” arXiv preprint arXiv:1611.07722, 2016.
- [15] J. Jow, Y. Xiao, and W. Han, “A survey of intrusion detection systems in smart grid,” International Journal of Sensor Networks, vol. 23, no. 3, pp. 170–186, 2017.[16] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, “A survey of distributed denial-of-service attack, preven- tion, and mitigation techniques,” International Journal of Distributed Sensor Networks, vol. 13, no. 12, p. 1550147717741463, 2017.
- [17] R. Mahmud, R. Vallakati, A. Mukherjee, P. Ranganathan, and A. Nejadpak, “A survey on smart grid metering infrastructures: Threats and solutions,” in 2015 IEEE International Conference on Elec- tro/Information Technology (EIT), pp. 386–391, IEEE, 2015.
- [18] I. Onyeji, M. Bazilian, and C. Bronk, “Cyber security and critical energy infrastructure,” The Electricity Journal, vol. 27, no. 2, pp. 52–60, 2014.
- [19] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. Al Ali, “Smart grid cyber security: Challenges and solutions,” in 2015 International conference on smart grid and clean energy technologies (ICSGCE), pp. 170–175, IEEE, 2015.
- [20] G. Wen, W. Yu, X. Yu, and J. Lu¨, “Complex cyber-physical networks: From cybersecurity to security control,” Journal of Systems Science and Complexity, vol. 30, no. 1, pp. 46–67, 2017.

Thank You

Prof. Amro M. Farid[1,2]

[1]-Thayer School of Engineering at Dartmouth
[2]-Department of Computer Science at Dartmouth

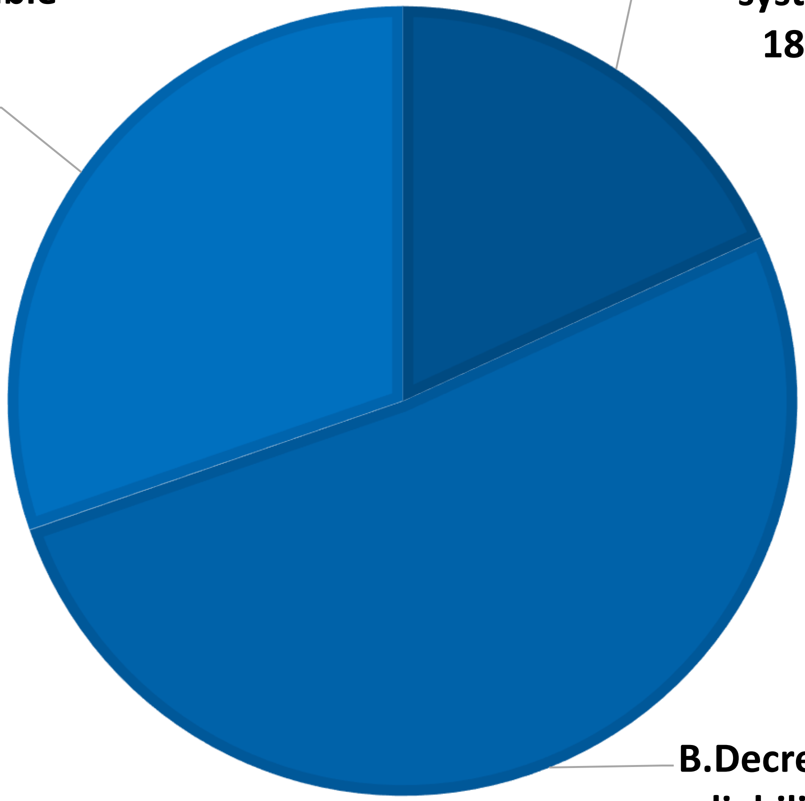
Email: amfarid_at_dartmouth_dot_edu

LIINES LABORATORY FOR INTELLIGENT INTEGRATED NETWORKS OF ENGINEERING SYSTEMS
EMPOWERING YOUR NETWORK

http://engineering.dartmouth.edu/liines

Polling Questions

1. If no changes to the current regulatory framework are done in the next ten years, do you think that decentralized resources in your country will?



2. In the power system of the future, which technology has the largest potential to increase power systems resilience?